II. AMENDMENTS TO THE CLAIMS

The following is a courtesy copy of the currently pending claims; no revisions have been made via this document:

1. (Previously Presented) System for back-up of data objects stored on a real smart card comprising:

a virtual smart card control component for handling creating of a virtual smart card and for providing the security and the read/write process for the virtual smart card;

a smart card manager component for providing a menu controlled graphical user interface allowing user actions for initiating creation of a VSC and back-up of data objects being stored in said real smart into said corresponding area of said virtual smart card; and

a communication component for transferring said data objects to be backed-up from said real smart card to said virtual smart card by using functionality of said virtual smart card control component.

2. (Previously Presented) System for secure copy of data objects being stored in a virtual smart card into a real smart card comprising:

a storage media for providing a virtual smart card having data objects to be securely copied into the assigned area of a real smart card;

a virtual smart card control component for handling creating of a virtual smart card and for providing the security and the read/write process for the virtual smart card (VSC);

a communication component for providing access to a real smart card via access to a

smart card driver assigned to the smart card reader and a card agent for providing smart card specific commands for writing said data objects to be securely copied from an intermediate buffer of said virtual smart card into said assigned area of said real smart card; and

a smart card manager component providing a menu controlled graphical user interface allowing to initiate user actions for creation of a VSC and secure copy of data objects being stored in said virtual smart card into said corresponding area of said real smart card.

3. (Previously Presented) System according to claim 1, wherein said communication component comprising:

a smart card API component providing an interface to said smart card manger component, an interface to said virtual control component, and an interface to a smart card & SC Reader Handler component providing an interface to all available smart card reader driver(s), wherein said smart card & SC Reader Handler has an interface to a smart card agency component providing an interface to all available smart card agent(s) providing smart card specific commands.

4. (Previously Presented) System according to claim 1, wherein said smart card API, said smart card manager component and said virtual smart card control component form an integral component.

5. (Previously Presented) A method to back-up of data objects being stored on a real smart card, characterized by the steps of:

opening and displaying data objects of the real smart card to be backed-up via a smart card manager graphical user interface;

selecting data objects to be backed-up via said smart card manager graphical user interface;

automatically creating a virtual smart card (VSC) by a smart card control component via said smart card manager graphical user interface, wherein said created virtual smart card having a defined logical file structure being identical with a logical file structure of said real smart card in use;

opening a data object area of said created virtual smart card for placing said data objects to be backed-up via said smart card manager graphical user interface;

copying data objects to be selected into said area of said created virtual smart card via said smart card manager graphical user interface; and

storing said virtual smart card on a secure permanent storage media.

6. (Previously Presented) Method according to claim 5, wherein said step for automatically creating of said virtual smart card comprises the following steps:

automatically creating a defined file structure having defined areas for placing data objects by a virtual smart card control program;

automatically assigning a password and an unique identifier to said defined file structure created and storing both in the respective area of said defined file structure by said virtual smart

card control program; and

electronically storing said defined file structure including said data objects on a storage media virtual smart card.

7. (Previously Presented) Method according to claim 6, wherein said defined file structure of said virtual smart card comprising:

a public area in which public data objects having no access conditions are placed;

a private area in which private data objects being encrypted are placed;

a secret key area in which key data objects being encrypted are placed;

a password area in which a password being encrypted is placed; and

an unique identifier area in which an unique identifier for identifying the VSC is placed.

8. (Original) Method according to claim 7, wherein said defined file structure of said virtual smart card is a dedicated file structure containing elementary files for defining the areas in which said data objects are to be placed.

9. (Original) Method according to claim 7, wherein user actions via said menu controlled graphical user interface with respect to the private areas of said virtual smart card require the input of a password.

10. (Original) Method according to claim 5, wherein said opening, copying, and storing steps are accomplished using a respective functionality provided by the virtual smart card control program.

11. (Original) Method according to claim 5, wherein said virtual smart card is created on a server system and is provided to a client system via a secure channel.

12. (Previously Presented) A computer program product stored on a computer usable medium comprising computer readable program means for causing a computer to perform the following method:

opening and displaying data objects of ~~a~~ the real smart card to be backed-up via a smart card manager graphical user interface;

selecting data objects to be backed-up via said smart card manager graphical user interface;

automatically creating a virtual smart card (VSC) by ~~said~~ a smart card control component via said smart card manager graphical user interface, wherein said created virtual smart card having a defined logical file structure being identical with a logical file structure of said real smart card in use;

opening a data object area of said created virtual smart card for placing said data objects to be backed-up via said smart card manager graphical user interface;

copying data objects to be selected into said area of said created virtual smart card via said smart card manager graphical user interface; and

storing said virtual smart card on a secure permanent storage media.